(19) BUNDESREPUBLIK DEUTSCHLAND

DEUTSCHES PATENT- UND MARKENAMT

(12) **Offenlegungsschrift**

(10) **DE 101 24 800 A 1**

(51) Int. Cl.[7]:
G 05 B 19/042
H 04 L 9/00

(21) Aktenzeichen: 101 24 800.8
(22) Anmeldetag: 21. 5. 2001
(43) Offenlegungstag: 12. 12. 2002

(71) Anmelder:
Siemens AG, 80333 München, DE

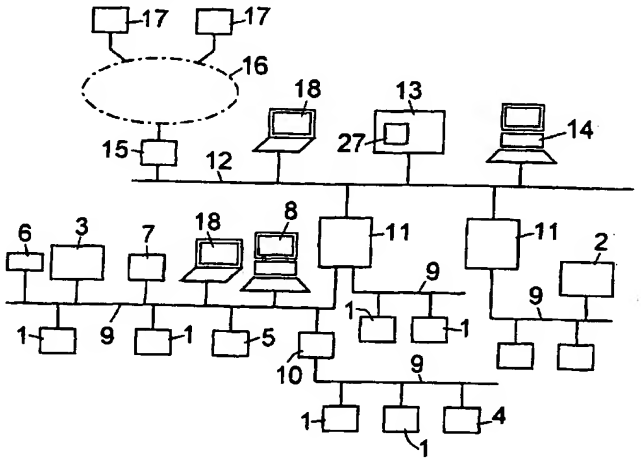
(72) Erfinder:
Kaszkin, Andreas, Dipl.-Ing. (FH), 91466 Gerhardshofen, DE; Stiehl, Wolfgang, Dipl.-Ing. (FH), 76744 Wörth, DE

Die folgenden Angaben sind den vom Anmelder eingereichten Unterlagen entnommen

Prüfungsantrag gem. § 44 PatG ist gestellt

(54) Prozessautomatisierungssystem und Prozessgerät für ein Prozessautomatisierungssystem

(57) In einem Prozessautomatisierungssystem, in dem Prozessgeräte (1 bis 6) vorgegebene Funktionen im Rahmen der Prozessautomatisierung ausführen und dabei mit dem Prozessautomatisierungssystem funktions- und/oder geräterelevante Daten (23, 24) austauschen, wird zumindest ein Teil der Daten (23, 24) verschlüsselt ausgetauscht.



DE 101 24 800 A 1

E 101 24 800 A 1

Beschreibung

[0001] Die Erfindung betrifft ein Prozessautomatisierungssystem und ein Prozessgerät für ein Prozessautomatisierungssystem.

[0002] In zunehmendem Maße ergibt sich die Forderung nach einer Übertragung von Daten zwischen einem Prozessautomatisierungssystem oder Teilen oder Komponenten davon und externen Stellen. Beispiele dafür sind Fernprogrammierung, Fernparametrierung, Fernwartung oder Ferndiagnose. So ist es aus der DE 198 48 618 A1 bekannt, zur Fernwartung und/oder Diagnose von der externen Stelle an das Prozessautomatisierungssystem zu übertragende Daten, z. B. ein Steuerbefehl, in eine E-Mail zu verpacken, diese an das Prozessautomatisierungssystem zu adressieren und dorthin abzusenden. Innerhalb des Prozessautomatisierungssystems wird die E-Mail von dem Adressaten empfangen, der den Steuerbefehl durch Decodieren extrahiert und an die Anwendung, für die der Steuerbefehl bestimmt ist, weiterleitet. Umgekehrt können in gleicher Weise Daten von dem Prozessautomatisierungssystem an externe Stellen übermittelt werden. Spezielle Datenverbindungen zwischen dem Prozessautomatisierungssystem und den externen Stellen sind dazu nicht erforderlich, weil standardmäßige Datenübertragungssysteme (globale und/oder lokale Datennetze, wie z. B. Internet bzw. Intranet) in Verbindung mit einem elektronischen Schutzwall (Firewall) um das Prozessautomatisierungssystem verwendet werden können, wobei der elektronische Schutzwall für die E-Mails durchlässig ist (sog. E-Mail-Tunneling).

[0003] Zur Erhöhung der Sicherheit gegen ein unerlaubtes Eindringen in den Schutzwall des Prozessautomatisierungssystems können die in der E-Mail verpackten Daten verschlüsselt und anschließend beim Extrahieren aus der E-Mail wieder entschlüsselt werden, bevor sie weitergeleitet werden. Dabei erfolgt die Verschlüsselung der an die externe Stelle zu übermittelnden Daten bzw. die Entschlüsselung der von der externen Stelle empfangenen Daten innerhalb des Prozessautomatisierungssystems in einer einzigen Verschlüsselungs- bzw. Entschlüsselungsvorrichtung. Es ist daher nicht ohne weiteres möglich, einen ausgewählten Teil der Daten, z. B. sicherheitsrelevante Daten, verschlüsselt und die übrigen Daten unverschlüsselt zwischen dem Prozessautomatisierungssystem und der externen Stelle auszutauschen. Statt dessen werden, soweit eine Verschlüsselung vorgesehen ist, alle über den elektronischen Schutzwall auszutauschenden Daten pauschal verschlüsselt, was mit einem entsprechenden Aufwand und einer Reduzierung der Datenübertragungsgeschwindigkeit verbunden ist. Ferner ist der Austausch der verschlüsselten Daten zwischen dem Prozessautomatisierungssystem und den externen Stellen auf den Weg über die Verschlüsselungs- und Entschlüsselungsvorrichtung in dem Prozessautomatisierungssystem beschränkt, so dass es nicht möglich ist, verschlüsselte Daten an unterschiedlichen Orten innerhalb des Prozessautomatisierungssystems zu kommunizieren. Schließlich sind zu sendende Daten vor ihrer Verschlüsselung und empfangene Daten nach ihrer Entschlüsselung innerhalb des Prozessautomatisierungssystems manipulierbar.

[0004] Die Verschlüsselung vertraulicher Daten vor ihrer Übertragung an einen Empfänger ist allgemein bekannt. Bei dem so genannten öffentlichen Verschlüsselungsverfahren verwendet der Sender einen öffentlichen Schlüssel des berechtigten Empfängers zur Verschlüsselung der Daten, so dass nur dieser die Daten mit seinem eigenen privaten Schlüssel entschlüsseln kann. Die Authentifizierung des Senders kann durch Signieren der Daten erfolgen. Dazu verschlüsselt der Sender die Daten mit seinem eigenen privaten

Schlüssel, während der Empfänger zur Entschlüsselung der Daten den öffentlichen Schlüssel des Senders verwendet. Mit öffentlichen Schlüsseln verschlüsselte Daten sind nicht notwendigerweise authentisch, während mit privaten Schlüsseln signierte Daten nicht vertraulich sind. Zur Herstellung von Vertraulichkeit und Authentizität können daher Verschlüsselung und Signierung kombiniert werden, wozu der Sender die Daten zunächst mit dem eigenen privaten Schlüssel und anschließend mit dem öffentlichen Schlüssel des Empfängers verschlüsselt. Um schließlich auch noch die Integrität, d. h. die Unverfälschtheit, der übertragenen Daten zu gewährleisten, kann der Sender aus den Daten einen Prüfcode bestimmen, der signiert, d. h. mit dem sendereigenen privaten Schlüssel verschlüsselt, an den Empfänger übertragen wird. Der Empfänger entschlüsselt den Prüfcode mit dem öffentlichen Schlüssel des Senders und vergleicht den so entschlüsselten Prüfcode mit dem aus den empfangenen Daten berechneten Prüfcode; wenn beide Prüfcodes gleich sind, ist die Integrität der Daten gesichert.

[0005] Der Erfindung liegt die Aufgabe zugrunde, eine flexible und zugleich sichere Handhabung ausgewählter wichtiger Daten eines Prozessautomatisierungssystems zu ermöglichen.

[0006] Gemäß der Erfindung wird die Aufgabe durch das Prozessautomatisierungssystem nach Anspruch 1 bzw. das Prozessgerät nach Anspruch 5 gelöst.

[0007] Vorteilhafte Weiterbildungen des erfindungsgemäßen Prozessautomatisierungssystems bzw. Prozessgeräts sind in den Unteransprüchen angegeben.

[0008] In dem erfindungsgemäßen Prozessautomatisierungssystem führen Prozessgeräte vorgegebene Funktionen im Rahmen der Prozessautomatisierung aus und tauschen dabei mit dem Prozessautomatisierungssystem funktions- und/oder geräterelevante Daten aus, wobei zumindest ein Teil der Daten verschlüsselt ausgetauscht wird.

[0009] Das erfindungsgemäße Prozessgerät für ein Prozessautomatisierungssystem enthält eine Funktionseinrichtung zur Ausführung vorgegebener Funktionen im Rahmen der Prozessautomatisierung und eine mit der Funktionseinrichtung verbundene und an das Prozessautomatisierungssystem anschließbare Kommunikationseinrichtung zum Austausch funktions- und/oder geräterelevanter Daten mit dem Prozessautomatisierungssystem, wobei die Kommunikationseinrichtung den Austausch zumindest eines Teils der Daten verschlüsselt durchführende Mittel aufweist.

[0010] Die Verschlüsselung bzw. Entschlüsselung von Daten erfolgt in den Prozessgeräten, also den Sendern und Empfängern der Daten, wobei die verschlüsselten Daten innerhalb des Prozessautomatisierungssystems auf dieselbe Weise wie unverschlüsselte Daten kommuniziert werden. Unter Prozessgeräten sind Feldgeräte, Wartengeräte und sonstige Endgeräte zu verstehen, also beispielsweise Messumformer, Aktoren, Antriebe, Analysengeräte, Steuerungen und Regler. So sind z. B. Messumformer Sender von Messdaten und Empfänger von Parametrierungsdaten, die zu ihrer Parametrierung dienen. In dem Umfange, in dem diese Daten als sicherungsbedürftig angesehen werden, werden sie über die Kommunikationseinrichtung des Messumformers verschlüsselt mit dem Prozessautomatisierungssystem ausgetauscht; andere, nicht als sicherungsbedürftig eingestufte Daten werden unverschlüsselt ausgetauscht. Je nach Verschlüsselung sind die verschlüsselten Daten gegen Manipulation geschützt und/oder können nur von einem berechtigten Empfänger empfangen werden, wobei zusätzlich der Sender authentifizierbar ist. Sender und Empfänger von Daten können gleichermaßen die Prozessgeräte innerhalb des Prozessautomatisierungssystems wie auch externe Stellen sein, die beliebig an das Prozessautomatisierungssystem an-

gekoppelt werden können.

[0011] In der Hardware, durch Programmierung oder durch ggf. verschlüsselt durchzuführende Parametrierung der Prozessgeräte ist festgelegt, welche Daten als sicherungsbedürftig gelten und verschlüsselt auszutauschen sind. So werden sicherungsbedürftige Sendedaten automatisch verschlüsselt, bevor sie abgesandt werden, und empfangene Daten können nur nach Entschlüsselung in dem Prozessgerät weiterverarbeitet werden. Dabei kann ein Teil der Daten sowohl unverschlüsselt als auch parallel dazu verschlüsselt ausgetauscht werden. Ein Beispiel hierfür sind Messdaten, die sowohl in dem Prozessautomatisierungssystem im Rahmen der Steuerung und Regelung unverschlüsselt weiterverarbeitet werden als auch bei eichpflichtigen Applikationen oder für amtliche Überwachungszwecke verwendet und dazu verschlüsselt werden. So können z. B. eichfähige Wägedaten von Industriewaagen verschlüsselt an einen externen Datenspeicher oder eine Anzeige ausgegeben werden, ohne dass der Datenübertragungsweg gekapselt werden muss, und gleichzeitig mit den unverschlüsselten Wägedaten beispielsweise ein Abfüllvorgang gesteuert werden. Da hier z. B. die verschlüsselten Daten im Wesentlichen für Registrierungszwecke verwendet werden, kann vorgesehen werden, dass die verschlüsselten Daten gegenüber den unverschlüsselten Daten nachrangig, d. h. mit niedrigerer Priorität, kommuniziert werden, so dass die Steuerung und Regelung mit den unverschlüsselten Daten nicht beeinträchtigt wird. Dabei kann insbesondere vorgesehen werden, dass verschlüsselte Daten zunächst, ggf. mit Zeitstempeln versehen, gesammelt werden, bevor sie zu einem späteren Zeitpunkt beispielsweise in einem Datenpaket gebündelt kommuniziert werden.

[0012] Zur weiteren Erläuterung der Erfindung wird im Folgenden auf die Figuren der Zeichnung Bezug genommen; im Einzelnen zeigen

[0013] **Fig.** 1 ein Ausführungsbeispiel des erfindungsgemäßen Prozessautomatisierungssystems und

[0014] **Fig.** 2 ein Ausführungsbeispiel des erfindungsgemäßen Prozessgeräts.

[0015] **Fig.** 1 zeigt in schematischer Darstellung ein Prozessautomatisierungssystem mit einer Vielzahl von Prozessgeräten, die vorgegebene Funktionen im Rahmen der Prozessautomatisierung ausführen und dabei funktions- und/oder geräterelevante Daten mit dem Prozessautomatisierungssystem austauschen. Unter Prozessgeräten sind hier Datenendgeräte, also Sender und Empfänger von Daten zu verstehen. Insbesondere gehören dazu Feld- und Wartengeräte, z. B. Messumformer **1** für Druck, Temperatur, Durchfluss, Füllstand usw., Analysengeräte **2** für Gas- oder Flüssigkeitsanalyse, Wägesysteme **3**, Stellungsregler für Ventile und sonstige dezentrale Regler **4**, Stellantriebe **5**, Registrier- und Anzeigegeräte **6**. Zum Austausch der Daten innerhalb des Prozessautomatisierungssystems sind die Prozessgeräte im dezentralen Peripheriebereich zusammen mit dezentraler Steuerung und Regelung **7** und Bedienung und Beobachtung **8** über Feldbusse **9** oder andere Kommunikationswege miteinander verbunden, wobei unterschiedliche Feldbusse **9** über Buskoppler **10** miteinander verbunden sind. Die Feldbusse **9** sind wiederum über Steuereinrichtungen **11** an einem zentralen Anlagenbus **12** angebunden, an dem auch eine zentrale Steuerung und Regelung **13** und Bedienung und Beobachtung **14** angeschlossen ist. Der Anlagenbus **12** ist über eine Koppeleinrichtung **15** mit einem globalen Kommunikationsnetz **16**, z. B. Internet, verbunden, um einen Datenaustausch mit externen Stellen **17** beispielsweise zur Fernwartung, -diagnose, -parametrierung, -überwachung usw. des Prozessautomatisierungssystems bzw. einzelner Prozessgeräte zu ermöglichen. Schließlich können weitere externe Stellen **18**, z. B. Programmier-, Diagnose- oder Servicegeräte an unterschiedlichen Punkten des Prozessautomatisierungssystems angekoppelt werden.

[0016] Vorgegebene sicherungsbedürftige Daten des Prozessautomatisierungssystems werden verschlüsselt ausgetauscht, wobei je nach Verschlüsselung sichergestellt ist, dass diese Daten auf dem Wege von dem Sender zu dem Empfänger oder den Empfängern gegen Manipulation geschützt sind und/oder nur von einem berechtigten Empfänger empfangen werden können, wobei zusätzlich der Sender authentifizierbar ist. Die Verschlüsselung bzw. Entschlüsselung erfolgt in den Datenendgeräten, also den Sendern bzw. Empfängern, hier den Prozessgeräten bzw. externen Stellen, wobei die verschlüsselten Daten innerhalb des Prozessautomatisierungssystems genauso wie unverschlüsselte Daten übertragen werden.

[0017] **Fig.** 2 zeigt ein Prozessgerät, hier z. B. einen Messumformer **1** mit einer Funktionseinrichtung **19** zur Ausführung der Messfunktion und mit einer mit der Funktionseinrichtung **19** verbundenen und an das Prozessautomatisierungssystem, hier den Feldbus **9**, anschließbaren Kommunikationseinrichtung **20** zum Austausch funktions- und/oder geräterelevanter Daten mit dem Prozessautomatisierungssystem. Die Funktionseinrichtung **19** umfasst einen Sensor **21** und eine Messwerterfassung und -berechnung 22, die Messdaten, Diagnosedaten und sonstige geräte- oder funktionsspezifische Daten **23** generiert und Befehls-, Parametrier- und sonstige ihr zugeführte Daten **24** verarbeitet. Diese Sendedaten **23** und Empfangsdaten **24** werden über die Kommunikationseinrichtung **20** des Messumformers **1** mit dem Prozessautomatisierungssystem ausgetauscht. Durch Hardwareverschaltung oder Programmierung ist festgelegt, welche der Sendedaten **23** in einer Verschlüsselungsvorrichtung **25** verschlüsselt werden. Bei Empfangsdaten **24** erkennt die Kommunikationseinrichtung **20**, welche der Daten verschlüsselt sind und entschlüsselt diese in einer Entschlüsselungsvorrichtung **26**. Die Verschlüsselung bzw. Entschlüsselung der Daten **23** und **24** erfolgt hier nach dem öffentlichen Verschlüsselungsverfahren. Dazu enthält jedes Prozessgerät, hier also der Messumformer **1**, einen eigenen privaten Schlüssel sowie einen dazu korrespondierenden öffentlichen Schlüssel, wobei die Schlüssel in dem Messumformer **1** hinterlegt oder von diesem selbst generiert werden. Im Unterschied zu dem unzugänglich abgespeicherten privaten Schlüssel wird der öffentliche Schlüssel bei der Einbindung des Messumformers **1** in das Prozessautomatisierungssystem, z. B. bei der Inbetriebnahme, einer zentralen Schlüsselverwaltung **27** (**Fig.** 1) mitgeteilt, für die ein separates Gerät vorgesehen sein kann oder die in einem bereits vorhandenen Gerät, z. B. einer speicherprogrammierbaren Steuerung, des Prozessautomatisierungssystems implementiert ist. Externe Stellen **18**, die mit Prozessgeräten Daten austauschen wollen, melden sich zuvor automatisch bei der Schlüsselverwaltung **27** an und hinterlegen dort nach Überprüfung ihrer Identität ihren jeweiligen öffentlichen Schlüssel. Die zentrale Schlüsselverwaltung **27** gewährleistet die Authentizität der verwalteten öffentlichen Schlüssel, indem diese jeweils mit dem privaten Schlüssel der Schlüsselverwaltung **27** signiert werden, so dass mit Hilfe des öffentlichen Schlüssels der Schlüsselverwaltung **27** jederzeit die Authentizität der öffentlichen Schlüssel geprüft werden kann.

[0018] Ist z. B. vorgesehen, dass die Einstellung eines bestimmten Parameters in einem Prozessgerät, z. B. 4, nur durch eine autorisierte externe Stelle **18** möglich sein soll, so wird der an das Prozessgerät **4** zu übertragende Einstellwert in der externen Stelle **18** derart verschlüsselt, dass die Integrität des Einstellwerts beim Empfang durch das Pro-

zessgerät **4** sichergestellt ist und dass ferner das Prozessgerät **4** die Identität der externen Stelle **18** und damit deren Berechtigung zur Parametereinstellung feststellen kann.

[0019] Es kann vorgesehen sein, dass ein und dieselben Daten, hier z. B. die Messdaten des Messumformers **1**, an bestimmte Empfänger, z. B. ein eichpflichtiges Registrier- oder Anzeigegerät, verschlüsselt und an andere Empfänger, z. B. die Messdaten weiterverarbeitende Regler, unverschlüsselt übertragen werden. In der Regel werden nur diejenigen Daten verschlüsselt übertragen, die sicherungsbedürftig sind; alle übrigen Daten, insbesondere die zur Prozesssteuerung und -regelung dienenden Daten, werden überwiegend unverschlüsselt übertragen. Um die Prozesssteuerung und -regelung nicht zu beeinträchtigen, werden die unverschlüsselten Daten mit höherer Priorität als die verschlüsselten Daten kommuniziert, wozu die verschlüsselten bzw. zu verschlüsselnden Daten zunächst in einem Speicher **28** des Prozessgeräts **1** gesammelt werden können.

[0020] Die hier beschriebene Datenverschlüsselung ermöglicht also insbesondere eine fälschungssichere Fernparametrierung von Prozessgeräten oder einen autorisierten Service von beliebigen Stellen aus, eine sichere amtliche Überwachung von Messwerten oder Prozesszuständen, eine fälschungssichere Übertragung von sicherheitsrelevanten und/oder vertraulichen Daten, Diagnosedaten oder Anlagenparametern, wie z. B. Rezepturen, die Übertragung von eichfähigen Daten ohne das Erfordernis einer Kapselung der Übertragungswege, uvm.

Patentansprüche

1. Prozessautomatisierungssystem, in dem Prozessgeräte (**1** bis **6**) vorgegebene Funktionen im Rahmen der Prozessautomatisierung ausführen und dabei mit dem Prozessautomatisierungssystem funktions- und/oder geräterelevante Daten (**23**, **24**) austauschen, wobei zumindest ein Teil der Daten (**23**, **24**) verschlüsselt ausgetauscht wird.

2. Prozessautomatisierungssystem nach Anspruch 1, dadurch gekennzeichnet, dass zumindest ein Teil der Daten (**23**, **24**) verschlüsselt und parallel dazu unverschlüsselt ausgetauscht wird.

3. Prozessautomatisierungssystem nach Anspruch 1 oder 2, dadurch gekennzeichnet, dass verschlüsselte Daten gegenüber unverschlüsselten Daten nachrangig ausgetauscht werden.

4. Prozessautomatisierungssystem nach Anspruch 3, dadurch gekennzeichnet, dass verschlüsselte Daten zunächst in einem Speicher (**28**) des Prozessgeräts (**1**) gesammelt und danach ausgetauscht werden.

5. Prozessgerät (**1**) für ein Prozessautomatisierungssystem mit einer Funktionseinrichtung (**19**) zur Ausführung vorgegebener Funktionen im Rahmen der Prozessautomatisierung und mit einer mit der Funktionseinrichtung (**19**) verbundenen und an das Prozessautomatisierungssystem anschließbaren Kommunikationseinrichtung (**20**) zum Austausch funktions- und/oder geräterelevanter Daten (**23**, **24**) mit dem Prozessautomatisierungssystem, wobei die Kommunikationseinrichtung (**20**) den Austausch zumindest eines Teils der Daten (**23**, **24**) verschlüsselt durchführende Mittel (**25**, **26**) aufweist.

Hierzu 1 Seite(n) Zeichnungen

- Leerseite -

Nummer: DE 101 24 800 A1
Int. Cl.[7]: G 05 B 19/042
Offenlegungstag: 12. Dezember 2002

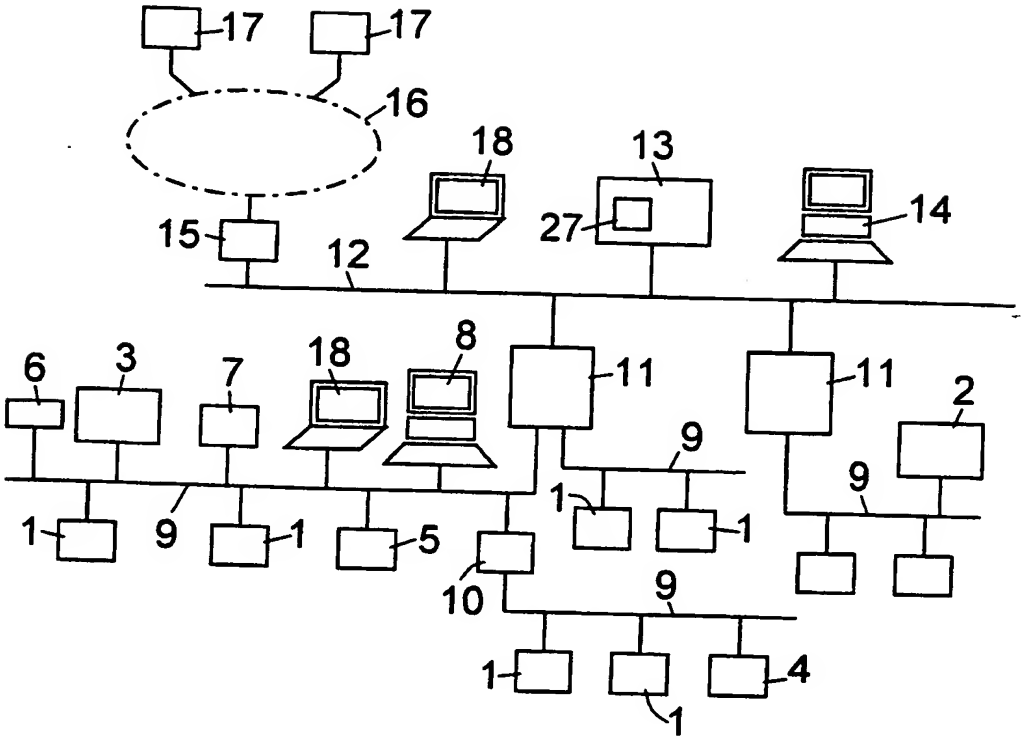


FIG. 1

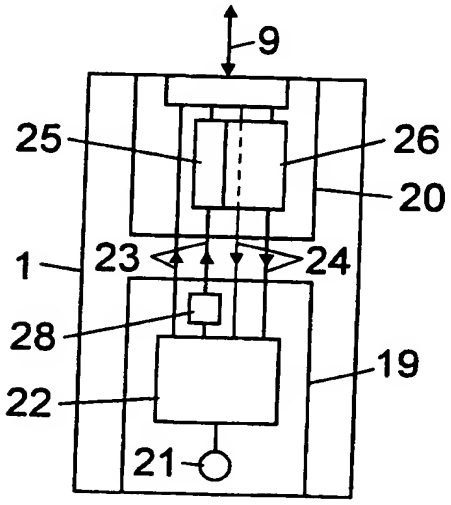


FIG. 2